

Identities and Devices

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks
- Twitter @DrAzureAD
- MVPx2 & MVR



NORDIC

— VIRTUAL SUMMIT —

Identities and Devices

The Foundation of Azure Active Directory Security

*“identity becomes the new
security perimeter”*

- Patrick Harding (2013), CTO, Ping Identity

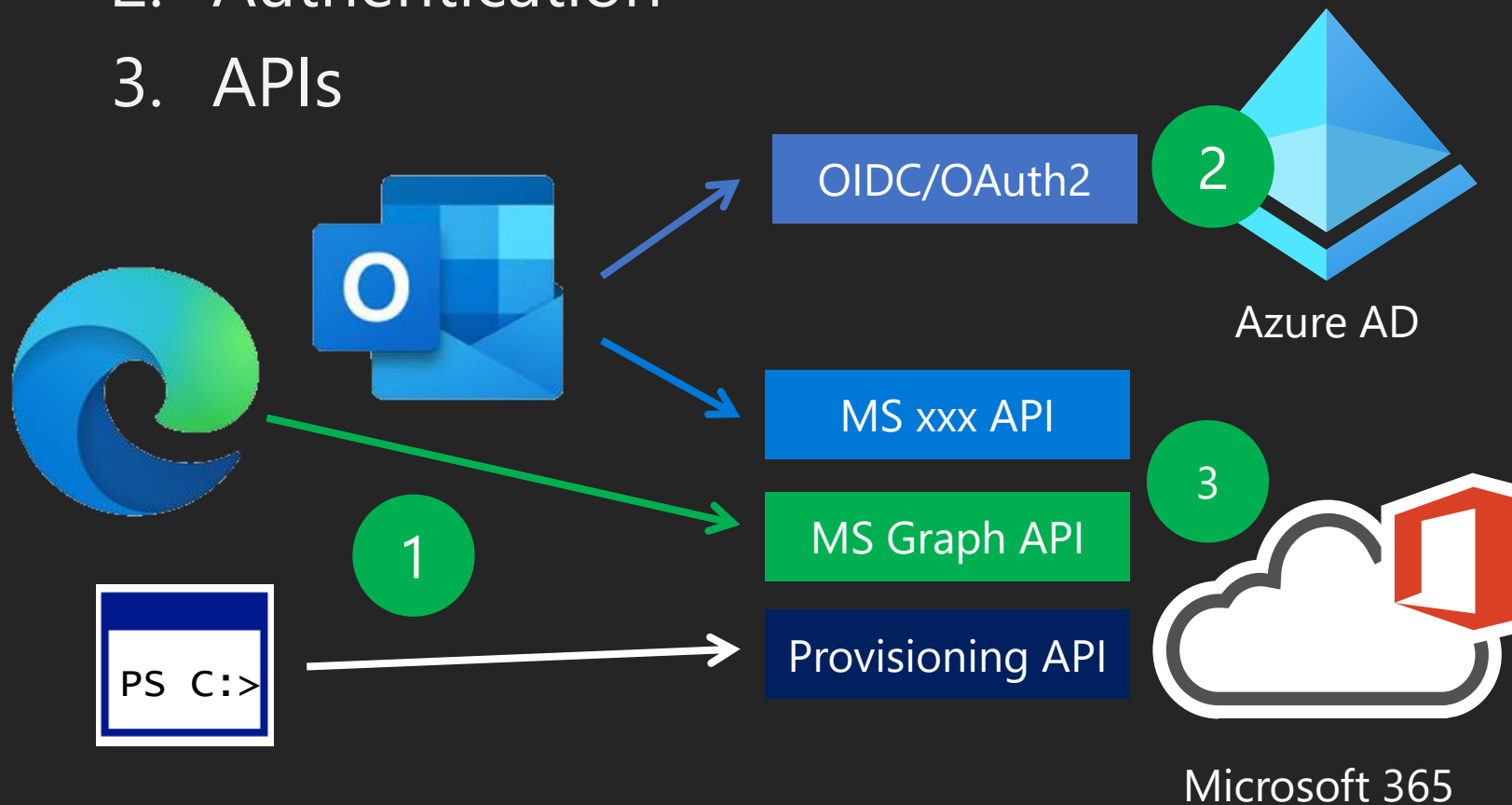
Contents

- Introduction
- How to protect users' identities?
- How to protect organisation?

Introduction

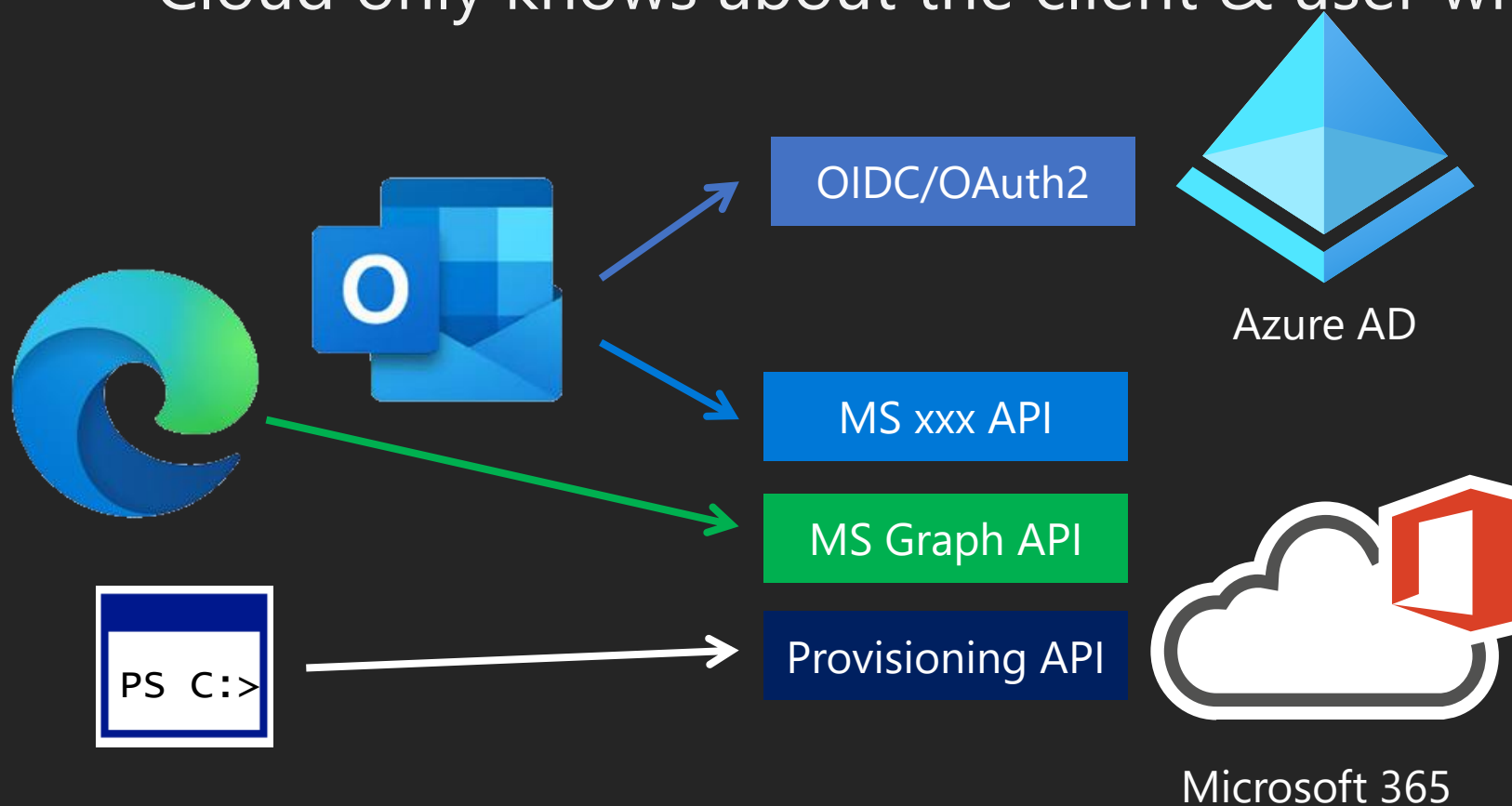
How the cloud works? 1/2

1. Clients
2. Authentication
3. APIs

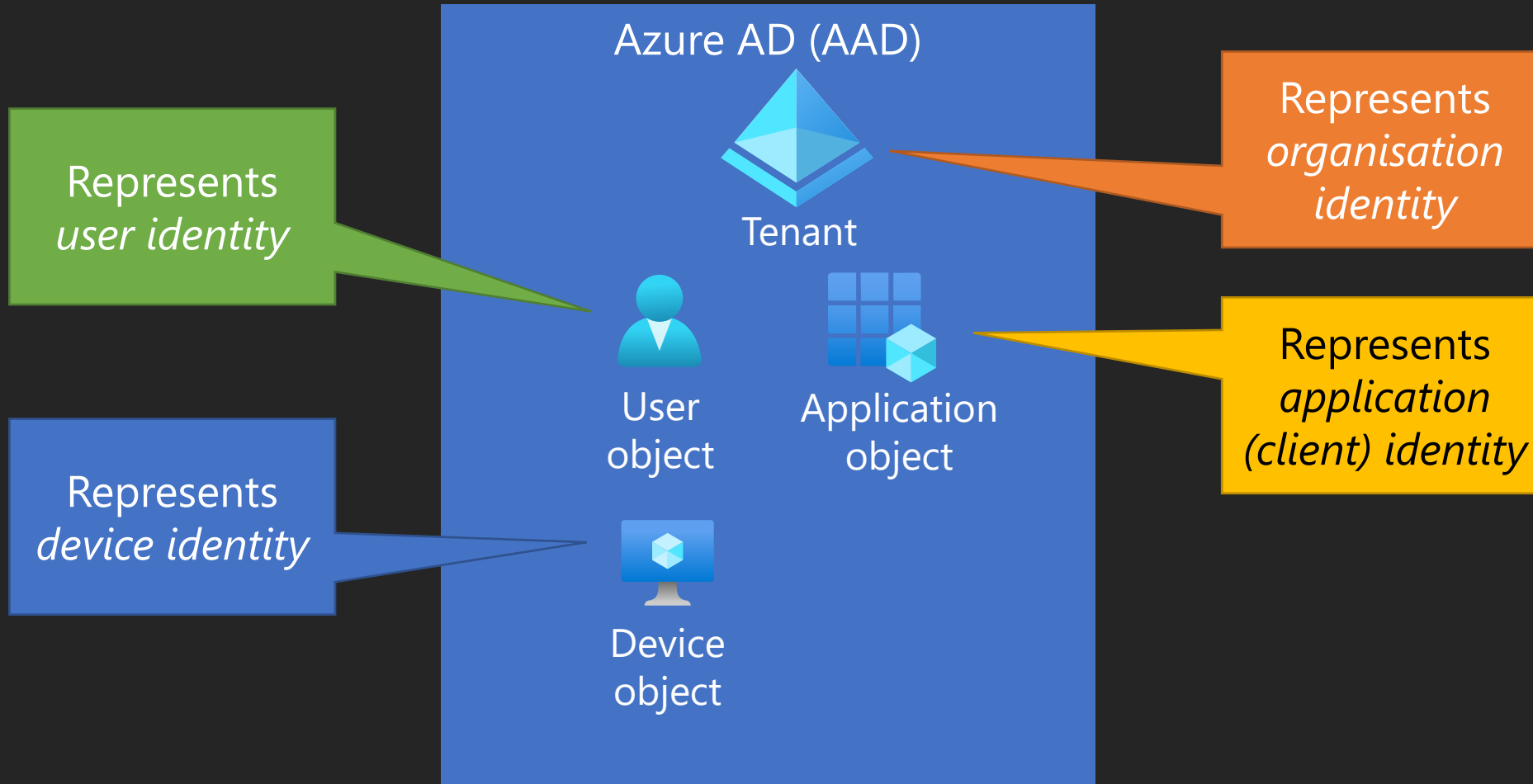


How the cloud works? 2/2

- Cloud (only) does what client tells it to do!
- Cloud only knows about the client & user what it is told to!



Introduction to identities



Proof of identity

Proof of identity	User	Device	App/client
Username + password (ROPC)	X		X
Authenticator	X		
FIDO2	X		
Kerberos ticket (Seamless SSO)	X		
SAML token (federated identity)	X		
Primary Refresh Token (PRT)	X	X	
Refresh token	X	X	
Windows Hello for Business	X	X	
Certificate		X	X

How to protect users' identities?

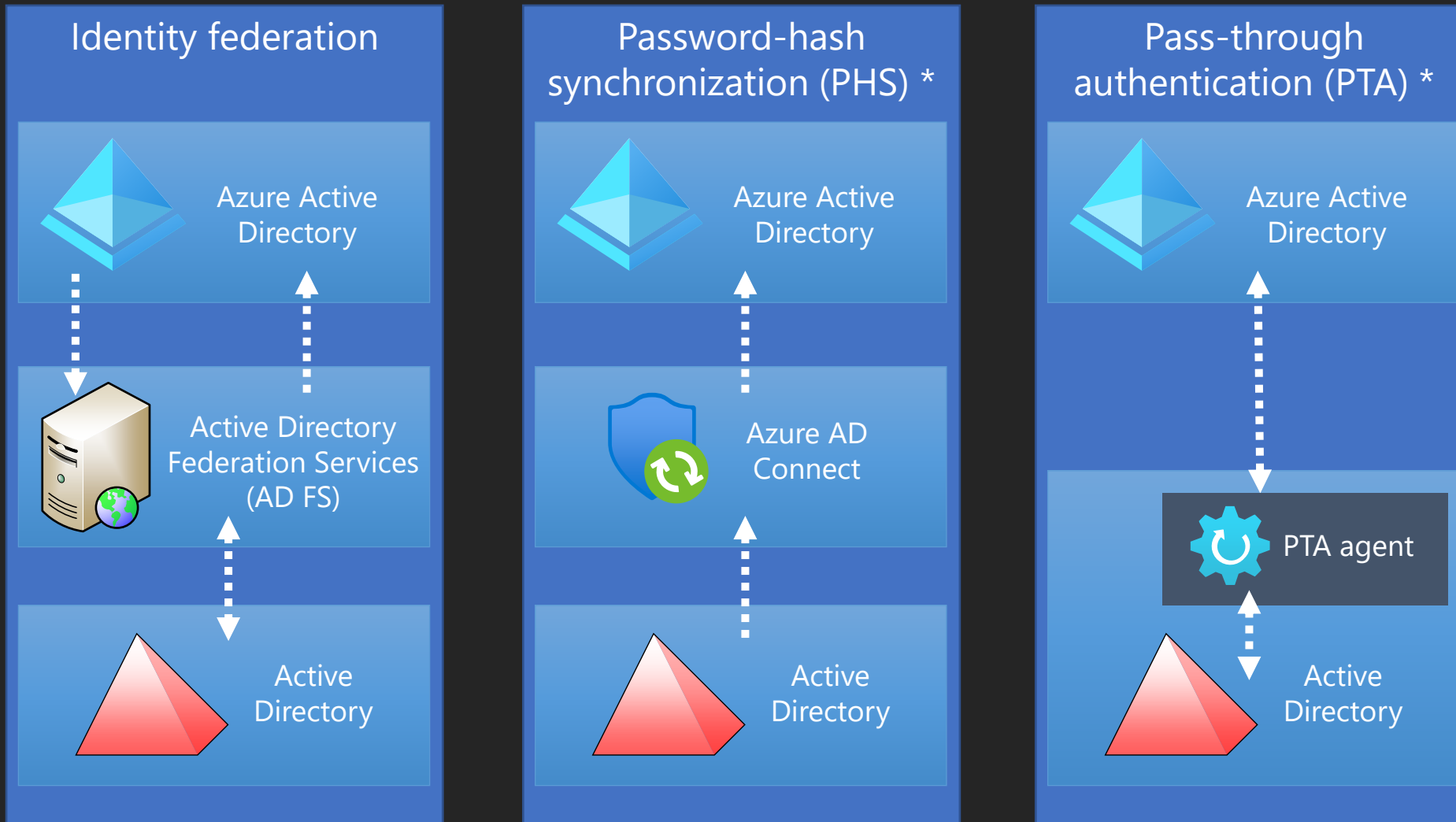
How to protect users' identities?

- Identity is the ~~new~~ security perimeter we need to focus on
- Only way to access the cloud is using identities

To protect users' identities:

1. Use Multi-Factor Authentication (MFA)
2. Protect the source of authority (if hybrid)

Hybrid authentication options



Demo!



How to protect organisation?

How to protect organisation?

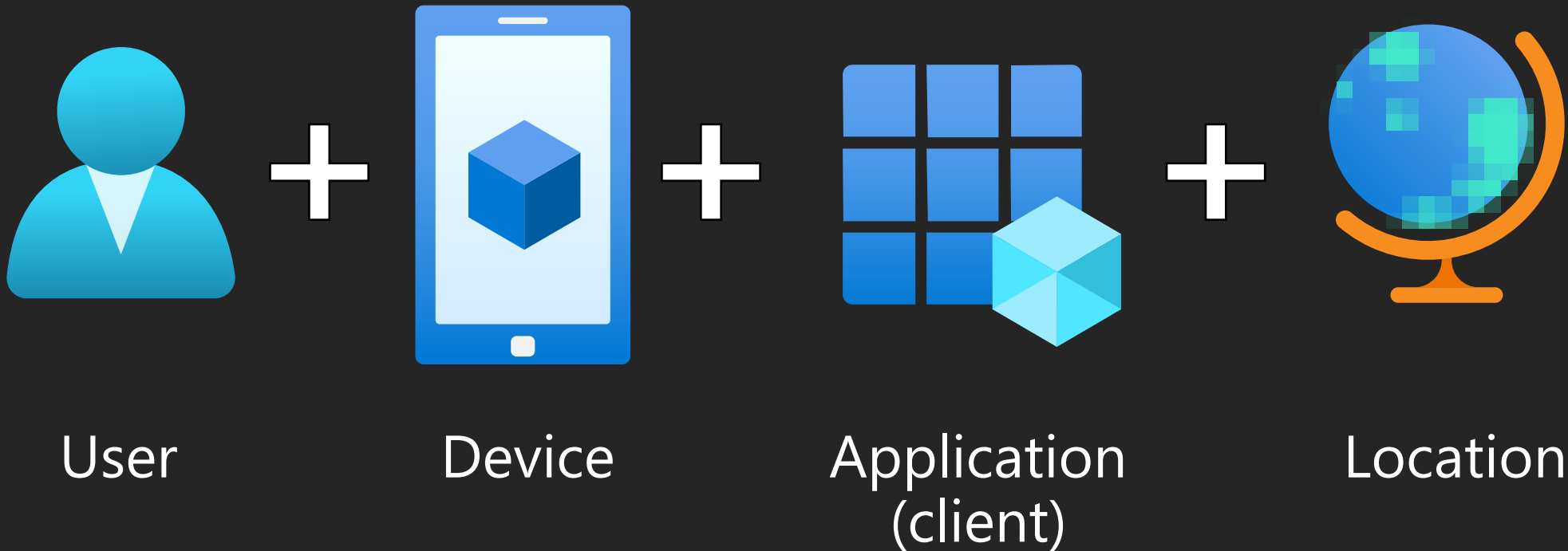
- Protecting (only) identities, doesn't protect the organization!
- The endpoint where cloud is accessed needs to be protected too!

To protect organization:

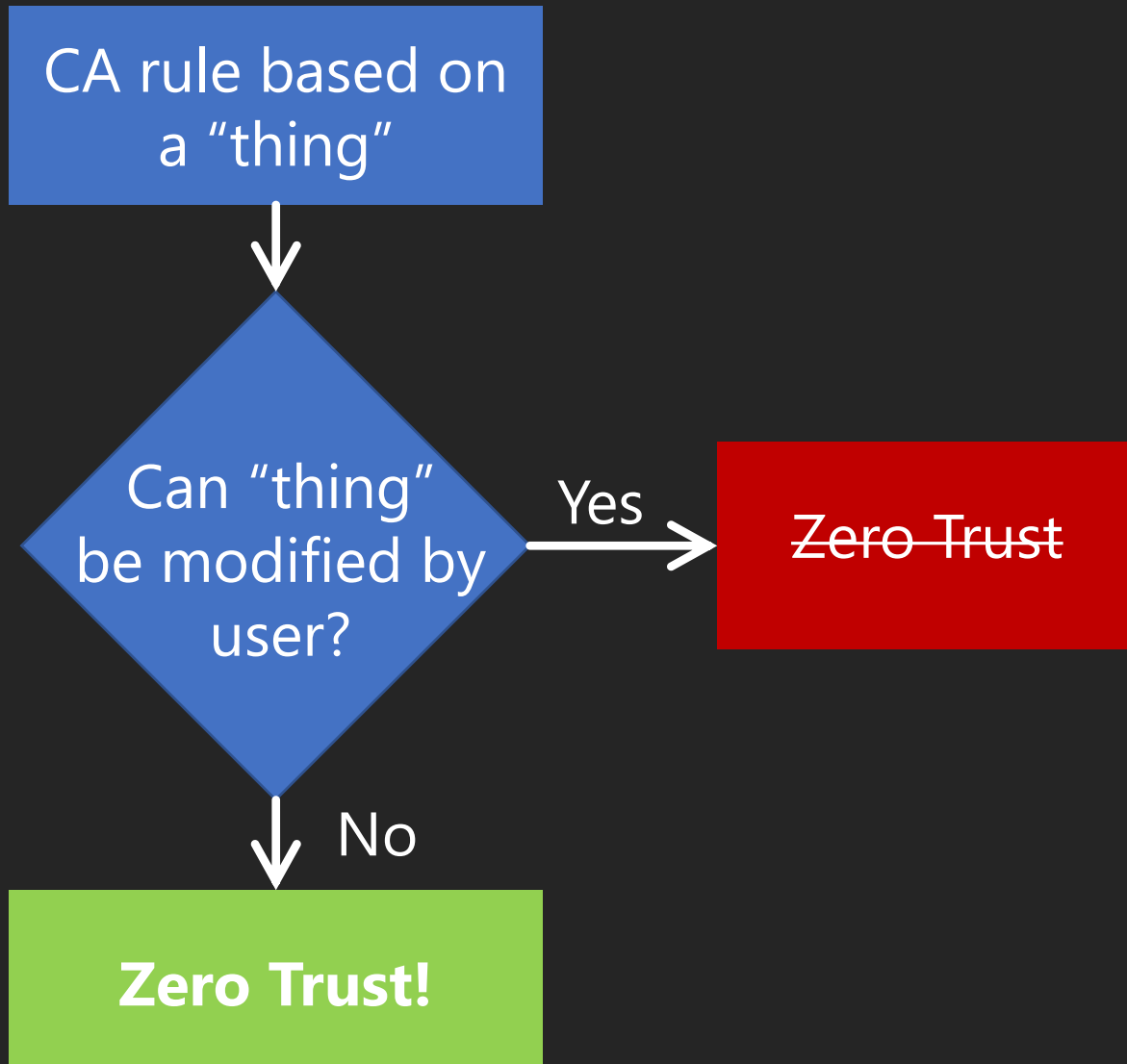
1. Use Conditional Access
2. Apply **real** Zero Trust!

Conditional Access

- Grant / block access based on conditions
- Outside signals:



Zero Trust flowchart for CA



Demo!



Summary

To protect identities and organization:

- Use **MFA**
- Allow access **only** from managed & compliant devices
- Do not allow **users** to join devices

Thank you!

Join me in MSRC researcher panel Nov 17th: <https://aka.ms/MSRC-Registration>



Follow me!

@DrAzureAD